HMIS Data and Technical Standards

National Broadcast

October 18, 2004

Topics Covered During the HMIS Broadcast

1. Introduction to the HUD HMIS Strategy
2. Universal and Program-Specific Data Elements
3. Privacy Standards
4. Security Standards
5. Guidance on Implementation

HMIS and Congressional Direction

- Congress directed HUD to provide data and analysis on the extent and nature of homelessness and the effectiveness of the McKinney Act programs including:
  - Developing unduplicated counts of clients served at the local level;
  - Analyzing patterns of service use; and
  - Evaluating the effectiveness of these systems

Progress toward HMIS Implementation

- October 2004 Goal
- Publication of Final Notice
- First Annual Homeless Assessment Report

Goal of October 2004

- "Goal" as HUD recognizes the considerable planning and work required to put in place an effective HMIS system
- Beginning in 2003, HMIS became a competitively rated component of the SuperNOFA application

HMIS Data and Technical Standards Notice

- Applies to:
  - Recipients of HUD McKinney-Vento Act program funds (ESG, SHP, S+C, Section 8 Mod Rehab for SRO)
  - HOPWA projects that target homeless persons
- HUD encourages participation of other federal programs that serve homeless persons

Annual Homeless Assessment Report (AHAR)

- HUD’s response to Congressional directive
- Sample of 80 communities
- Timeframe for Data Collection for 1st AHAR: Feb.–Apr. 2005
- Reporting Requirements

Close Encounters with the Data Standards

Why Uniform Data Standards?

- Local Use
  - Identify service and resource needs across providers and report to funders
  - Provide precise safeguards to protect client information
- National Use
  - AHAR
  - Report program achievements to Congress and public

Developing the HMIS Notice

- Input from Expert Panel of Providers, Researchers, HMIS Experts – August 27-28, 2002
- Draft Notice July 22, 2003
- Comment Period through September 22, 2003
- Final Notice July 30, 2004

Components of HMIS Standards

- Universal Data Elements
  - All providers, all clients
  - Understand extent, characteristics, and patterns of service use
- Program-Specific Data Elements
  - Mandated for McKinney-Vento programs
  - Record needs assessments and report outcomes
- Privacy, Security and Technical Standards

Key Decisions in Final Notice

- Definitions/response categories are uniform, but data collection is flexible
- Data sharing among providers within a CoC is encouraged but not mandated
- Priorities for adding providers begin with emergency, transitional, and outreach

Key Decisions in Final Notice

- Domestic violence programs participate, with special provisions
- Privacy and security standards are in two tiers: mandatory baseline standards and optional standards

Universal Data Elements

- Kept to minimum to reduce burden on homeless service providers
- Needed to create an accurate unduplicated count—cannot do it without personal IDs
- Needed to understand dynamics of homelessness—program entry and exit

Universal Data Elements

1. Name
2. Social Security Number
3. Date of Birth
4. Ethnicity and Race
5. Gender
6. Veterans Status
7. Disabling Condition
8. Residence Prior to Program Entry
9. Zip Code of Last Permanent Address
10. Program Entry Date
11. Program Exit Date
12. Person ID Number
13. Program ID Number
14. Household ID Number

Universal Data Elements: Disabling Condition

- Needed to determine which clients are chronically homeless and to learn more about their service patterns
- Several ways to collect information
- Unless required for program eligibility, must wait until after intake to ask

Universal Data Elements: SSN, Ethnicity, and Race

- Unless SSN is required by a program, a provider may not refuse service to someone who refuses to give an SSN

- Ethnicity and race follow OMB standards

Universal Data Elements: Prior Residence

- HMIS → APR response categories
- Applies to night before admission

Program-Specific Data Elements

1. Income and Sources
2. Non-Cash Benefits
3. Physical Disability
4. Developmental Disability
5. HIV/AIDS
6. Mental Health
7. Substance Abuse
8. Domestic Violence
9. Services Received
10. Destination
11. Reasons for Leaving
12. *Employment*
13. *Education*
14. *General Health Status*
15. *Pregnancy Status*
16. *Veteran's Information*
17. *Children's Education*

Program-Specific Data Elements (cont.)

- Collected from all clients served by programs that report this information to HUD
- Needed to assess the operations and outcomes of programs
- Related to APR response categories
- Include some non-APR data elements

Privacy Standards

Privacy Standards

- Three HMIS Privacy Challenges
- Fair Information Practices
- Ideas for Proceeding

Privacy Challenge 1

- Challenge: Broad diversity of Covered Homeless Organizations (CHOs) with differing programmatic and organizational realities

- Solution: <u>One size does not fit all</u>

  Baseline standards with local options

Privacy Challenge 2

- Challenge: Some organizations may have records subject to HIPAA
- Solution: HMIS privacy rules do not apply if a CHO determines that a substantial portion of its records about homeless clients or homeless individuals is covered by HIPAA

Privacy Challenge 3

- Challenge: What does *privacy* mean?

- Solution: <u>Fair Information Practices</u>

  Openness, Accountability, Collection Limitation, Purpose and Use Limitation, Access and Correction, Data Quality, and Security

Defining Privacy

- Rules about collection, maintenance, disclosure, and use of *personal information*

- Fair Information Practices *(FIPs)*: Principles for the processing of personal information that will enhance data protection

FIPs # 1 Openness

- Written policy is the vehicle for making, amending, publishing privacy rules
- Binding
- Post sign about policy
- Available to all on request
- Publish on webpage (if maintained)

FIPs # 1 Openness

Additional Privacy Protections

- Try to give a copy to each client
- Give a copy to each client
- Advance notice of amendments, prospective application of amendments, public comments

FIPs #2 Accountability

- Accept and consider complaints
- Confidentiality agreement for staff

FIPs #2 Accountability

Additional Privacy Protections

- Privacy training for staff
- Privacy policy compliance review
- Appeal process for denial of access or correction complaint
- Designate a Chief Privacy Officer

FIPs #3 Collection Limitation

- Collect PPI only when appropriate to the purposes or required by law
- Use lawful and fair means
- When appropriate, collect PPI with knowledge or consent of data subject
- Post sign; infer consent for collection

FIPs #3 Collection Limitation

Additional Privacy Protections

- Restrict collection of PPI, other than required HMIS elements
- Collect PPI only with express knowledge or consent (unless required by law)
- Obtain oral or written consent

FIPS # 4 Purpose Specification and Use Limitation

- Notice must specify purposes for PPI collection and must describe all uses/disclosures
- CHO may use/disclose PPI only if allowed by the standard and described in the privacy notice.
- May infer consent for described uses/disclosures and for compatible uses/disclosures

FIPS # 4 Purpose Specification and Use Limitation (cont.)

- All uses/disclosures are permissive (except first party request or required by law)
- Uses/disclosures not specified in notice need written consent of the individual or legal requirement

Allowable Uses / Disclosures

- Provide or coordinate services
- Payment or reimbursement
- Administrative functions
- Create de-identified PPI
- Required by law
- Avert serious threat to health / safety
- About victims of abuse, neglect, DV
- Academic research
- Law enforcement

FIPS # 4 Purpose Specification and Use Limitation

Additional Privacy Protections

- Seek oral or written consent for use/disclosure
- Agree to requested restrictions on use/disclosure
- Limit use/disclosure to those in notice and necessary (not compatible) purposes

FIPS # 4 Purpose Specification and Use Limitation

Additional Privacy Protections (cont.)

- Not disclose PPI for national database
- Keep an audit trail for disclosures
- Make audit trails available to data subjects
- Limit disclosures to minimum necessary

Ideas for Implementation 1

- Consult throughout with affected offices, staff, client representatives
- Prepare input-output chart for PPI
- Find other applicable requirements (state laws; HIPAA?)
- Start drafting policy from baseline, evaluate extras

Ideas for Implementation 2

- Identify necessary changes in operating procedures (e.g., access/correction)
- Staff Training/Confidentiality Agreement
- Don’t forget contractors, volunteers, other affiliates

10 Minute Break

HMIS National Broadcast

October 18, 2004

Security Standards

Security Standards

- Which of our computers/ systems are affected ("Applicability")?
  - *All* workstations, desktops, laptops, servers connected to the CHO network
  - This includes remote users accessing a Virtual Private Network (VPN)

Authentication

Minimum:

- Passwords with at least one number and one letter
- Not based on user's name, organization, or software
- Not based on common words

– Good: [Na$car#39]

– Bad: bobclark99

– Terrible: hmis

Passwords

"Written information pertaining to user access should not be stored or displayed in any publicly accessible location"

- *No PostIt Notes!*

Multiple Access

An individual user account should not be allowed access to HMIS from multiple workstations on the network at the same time.

- On Windows/Novell Networks, this can be enforced internally via a simple domain policy

Virus Protection

All systems on the network (including remote and VPN users) must have anti-virus software installed and updated regularly.

Old anti-virus software

=

No anti-virus software

Firewalls

The risk of accessing HMIS from a machine that also connects to the Internet is that usernames, passwords, and confidential data can all be compromised.

Firewalls (cont.)

- All machines accessing HMIS must have firewall protection from public networks (i.e., the Internet), typically via hardware.
- Any machines accessing the Internet via dial-up modem must have a personal firewall, typically via software.

Public Access

- HMIS that use public forums for data collection/reporting must have additional security to limit access, through *digital certificates* using standard Public Key Infrastructure (PKI).
- Digital certificates must be self-signed or signed from a trusted 3rd party (e.g., Verisign, Thawte).
- Translation: Any Web-based HMIS accessed over the Internet, needs digital certificates installed on all browsers accessing it.

Public Access (cont.)

Non-web based systems that transmit over the Internet (e.g., Microsoft DCOM / RDC or CORBA client-server desktop technologies) <u>also</u> require strong encryption to protect confidential data, and PKI certificates to verify the user.

- Example: Microsoft Terminal Services and Citrix may not enable encryption by default.

Physical Access

"When workstations are in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals"

- Screensavers with passwords (Windows/Mac)
- Session Timeout/Auto-logout (Web)
- Terminal Lock (Mainframe)

Backup and Disaster Recovery

All HMIS data must be regularly backed up and stored in a secure off-site location:

- **Backup your data and applications**
- **Save them to tape**
- **Test the tapes**
- ***A Backup tape laying next to a server won't help if the server room catches fire!***
- **Alternatively, consider secure network-based offsite backup solutions**

Secure Disposal

- – Tapes, disks *and* hard drives must be properly formatted and erased before disposal.
  - • At least two erasure passes (three more more is recommended)
- – Free and commercial software is available to prepare old workstation hard drives, tapes, and floppies before discarding.

System Monitoring

- Both accessing systems and central servers must be monitored *and* “routinely” reviewed by staff.
  - Warning: Many default operating system installations (e.g., Windows 2000) have rich logging *disabled* by default, making servers connected directly to the Internet or to an enterprise LAN especially vulnerable.

Default Installations

Most major operating systems (Microsoft Windows, Mac OSX, Linux, Solaris) have *very* insecure default installations. Particularly for servers connected directly to the Internet, special precautions *must* be taken to ensure data are protected.

- Excellent resource: “Hardening Windows 2000” (also applies to XP)

  http://www.systemexperts.com/literature.html

Application Security

- – *Both* the workstation and the software used to access HMIS data should require user authentication (e.g., passwords)
- – Logging on to the HMIS computer alone is not sufficient

Data Encryption

- All data transmitted over *publicly accessible networks* must:
  - Encrypt data (128 bit)
  - Verify user via digital certificates

Help from the Experts: Best Practices

- SANS Institute: Top 20 Security Vulnerabilities
  - http://www.sans.org/top20/
- Carnegie Mellon/CERT: Connecting to the Internet
  - http://www.cert.org/tech_tips/before_you_plug_in.html
- CERT Implementation Tips for Servers and Networks:
  - http://www.cert.org/tech_tips/
- Microsoft Security How-to Resources
  - http://www.microsoft.com/technet/itsolutions/howto/sechow.mspx

Implementing the Final Notice

Implementing the Final Notice

- Security Requirements
  - Implement security standards to reduce “human error”
- Privacy Requirements
  - Develop and/or update HMIS Policies and Procedures that require human commitment and action to a process

The Importance

- The success of any HMIS implementation hinges upon every user of the system being able to:
  - Communicate to a client the benefit of participation in the HMIS and what is happening with their personal information;
  - Understand the bigger picture of why they are collecting and entering information into the HMIS; and
  - Adhere to the policies and procedures established for operation of the HMIS.

Requirements

- All organizations participating in the HMIS must meet the baseline privacy and security requirements described in the final notice.

What do I need to do at the local level to be compliant?

- Final Notice sets requirements that will affect:
  - Homeless Service Provider / Organizations
  - System Administrators / HMIS Project Managers
  - Solution Providers / Developers / Database Hosts
  - Continua of Care

CoC Requirements

- Must designate a central coordinating body that will be responsible for centralized collection and storage of data
- HMIS data must be collected to central location at least once a year from all HMIS users within the CoC
- HMIS data must be stored for a minimum of 7 years
- Assure compliance with federal, state, and local confidentiality protections

CoC Action Steps

- Establish or task an HMIS committee or working group to develop, implement, and monitor compliance with the Final Notice at the local level
  - This group should also develop and/or update the Policies and Procedures for operation of the HMIS (including sample client notification, sharing agreements, user training protocols, etc.)
- It is also recommended that each CoC designate at least one person to become the Data and Technical Standards EXPERT

Covered Homeless Organization (CHO) Requirements

- Data Collection
- Privacy Policies
- Technical Requirements
- Data Access, Transmission, and Storage

Data Collection

Requirements

- All programs must collect universal data elements
- All McKinney-Vento funded programs must collect program-specific data elements

Action Steps

- Update intake/ data collection forms to collect universal data
- Train intake workers/ case managers/ users on new data collection protocols
- Ensure system is capable of capturing these data

Privacy Policies

Requirements

- Verbal client notification
- Signed user agreement for compliance with privacy notice/policies

Action Steps

- Train users and data collection staff on new privacy policies
- Require all users to sign compliance agreement with privacy notice

Privacy Policies: Privacy Notice

Requirements

– Posted at intake/website
– Provided upon request
– Available in languages common in community
– Reasonable accommodations for people with disabilities
– Contain required elements

Action Steps

– Develop or revise privacy notice
– Post notice at intake desk and on web site
– Make notice available upon request to all clients
– Determine agency complaint protocol
– Establish protocol or verbal client notification

Technical Requirements

Requirements	Action Steps
– HMIS User authentication	– Update username/password protocol
– Virus protection	– Install updated virus software (with auto update) on all PCs
– Location specification	– Require all PCs accessing HMIS system to be staffed
– Password protected screen savers	– Configure each PC to turn password protected screen saver on automatically when left unattended
– Network or Individual Workstation Firewalls	– Ensure all networks and individual workstations accessing HMIS are protected by a firewall

Data Access and Handling Protocols

Requirements

- Secure hardcopy Personal Protected Information (PPI)
- Monitor user access logs

Action steps

- Implement agency procedure for securing all HMIS related documents that contain PPI
- System Administrator should implement regular schedule/protocol for monitoring user access

Data Transmission and Workstation Authentication

Requirements

- Industry standard encryption
- Workstation authentication
  - Public Key Infrastructure (PKI) certificate
  - Limit access based on IP address

Action Steps

- Ensure all data are transmitted with minimum 128 bit encryption (SSL)
- Work with software company to deploy certificate authority or limit access based on IP address

Data Storage and Removal Protocols

Requirements

- Data/equipment disposal
- Secure offsite data storage
- Binary data storage
- All servers must be stored in a secure, temperature controlled environment with fire and surge suppression systems

Action Steps

- Develop policies and procedures for data and equipment disposal
- Develop and test disaster protection and recovery plan
- Visit hosting location
- Ensure data stored in binary format and exportable in csv format

Additional security protocols

- **Optional privacy and security protections including:**
  - Written consent procedures
  - Offering copies of privacy notice
  - Designating a Chief Privacy Officer to supervise implementation
  - Applying a firewall to all HMIS workstations
  - Destroying HMIS media at a bonded vendor
  - All PPI are stored in an encrypted format

Conclusion

- The system is only as secure as the weakest link
- Access to all HMIS systems should be monitored and enforced
- Put in place as many technical solutions as possible to reduce the risk of human error

Resources

- Upcoming white papers
- Shared forms and templates (e.g., Privacy Notice, Client consent forms)
- Crosswalk between HMIS and APR
- Further technical assistance

Feedback on Today's Broadcast

- We need your feedback on this broadcast to plan future guidance on this topic

- Please complete the online survey at: www.abtassociates.com/HMIS_broadcast

- You may also send comments to: BroadcastFeedback@abtassoc.com